Global Information Assurance Certification Paper

Preventing Piracy

Kevin Burke

GSEC Version 1.2f

Introduction

Computer software is a big business. Many companies rely on the sale of their software as their main or only source of income. For this reason companies must protect these assets just like any other asset in the company. Software piracy can cost a company a lot of money in lost sales. To help prevent this companies are doing many things. I will cover some of the different approaches that companies are using to help to prevent this.

A company must start to be concerned with trying to protect their software long before it is released into the public. The source code for a program is generally one of the most important pieces of information that a software company has. Most vendors do not readily release their source code to the public. If they were to release it, then a competitor would be able to determine how that product was built and then incorporate it into their own product. One of the disadvantages of keeping the source code of products secret is that it is easier for a security hole to go undetected. If a malicious hacker is able to obtain it then they might be able to find security holes that the vendor is unaware of. A recent high profile example of this occurred on November 12, 2000 when someone hacked into Microsoft obtained the source code for an undisclosed product(s)[1].

This also brings up the point of espionage. If one company is able to steal another company's source code, then could put them years ahead of the game.

Unfortunately, it is not possible to lock up the source code of a particular product up forever. For a company to make money from the product they must make the product available to the customer in some form. Almost all modern software releases are compiled executables. This means that generally the source code is not released with the product. The consumer only sees the finished product.

Whatever form the product is released in, there is a certain amount of trust in the customer. How much trust the vendor puts in the hands of the customer varies greatly. Over the years there have been many different methods used to get the customer to pay for the product(s) that they are using. None of these

methods have totally disappeared, but instead many products combine several of these.

On My Honor …

One of the original models is called shareware. This model put implicit trust in the customer to pay for the software that was released. When a product was released it was meant to be shared with anybody and everybody freely. The idea was to get as many people to try it as possible. If someone did not like the product they were not required to pay for it. After a person has used the product for a certain period of time, usually 30 days, they were supposed to register it.

The main problem with this model is that there was very little that could be done to force the person to pay for it. One of the most common methods to try and stop using the program illegally was to make the product self-destruct, or stop working after trial ran out. This was easily circumvented, usually by deleting the program and reinstalling it. Another approach was to disable certain features in the free version that was supposed to be shared, and then tell everyone that certain additional features were available in full version. The problem with this was that many people would start to share the full version instead of the trial version.

Must Have Original

Many programs require the original every time the program starts up. This method has become very popular with personal applications such as games. These programs are designed to run on only one computer at a time, so it is possible to have the original installation media present every time the application starts up.

This system seemed to be a perfect solution. Most of these programs used CD-ROMs and at first it was difficult to duplicate. But in recent years CD writer have become commonplace. This means that someone can create a copy of the original CD and the computer will be unable to determine the difference from the original.

The Keys to the Kingdome

Networks have become a wonderful tool for businesses. They allow information and applications to be shared between different computers. They allow for all of the applications

that a user might want installed to be stored on a single computer. This prevents someone from having to keep track of a CD-ROM for each application that could be needed. This also stops one of the more popular methods of piracy protection, require the CD-ROM to install and to run the program. To help prevent rampant unauthorized installation of programs, they can require a key, usually printed on a sticker on the back of the CD-ROM case.

The main disadvantage to this system is that as long as someone has a valid key, no matter whose key it is, is able to install the program. There are many generic keys that can be readily obtained on the Internet. This method only begins to become strong when coupled with other means of protection.

E.T. Phone Home

The latest step in piracy prevention methods takes some of the work away from the end user. In order for the product to become fully functional the application vendor must be contacted. Depending on the product you can either give them proof of purchase, such as a key that came with the product or when this is used with a shareware model, you must pay to obtain the key.

One example of such a product is SolidWorks, produced by SolidProducts. Once the product is purchased a email or fax must be sent to SolidProducts with information such as the users name, address, phone, and the serial number which came with the product. A registration code will be sent back that can be entered into the product. SolidWorks will run for 30 days before the registration code is required[2]. WinZip allows a user to use the product free for 30 days before they are required to register it. The registration process includes submitting personal information, such as name, address, etc. It also includes payment for the product[3].

Microsoft has come out with the latest twist on this technology. Both Windows XP and Office XP need to be activated before they can become fully functional. Windows XP for example must be activated within 30 days of installation otherwise it will become nonfunctional. The activation process consists of a unique computer ID, derived from the unique serial number provided with the documentation, and a hash of the current hardware configurations are sent to Microsoft and an installation ID being entered back into the local computer[4]. If there are multiple activations requests that have different hardware hashes but the same computer ID then it is likely that

the software is being installed on multiple machines. This particular system is designed to prevent limited end user piracy, but is not intended to protect against large-scale piracy[5].

There are several disadvantages to this system. Many people are especially displeased with the method that Microsoft uses, where it looks at the users machine. Some people do not like the idea of having their software contacting its vendor[6]. What the product is actually doing does not make a difference, it is what the customers think the product is doing which can hurt it. The other disadvantage is that this requires extra resources be set aside for an extended period of time in order to ensure that a customers product is rendered useless, possibly as long as the company is in business.

What I Have

The final type of software protection that I will discuss is where there is something that is physically attached to the computer. This comes in two distinct flavors hardware drivers or utilities and a dongle attachment. The software drivers and utilities are usually designed to support a particular piece of hardware, such as a sound card. Generally these are distributed freely because they are designed to run on a particular model of a particular vendors card, and will probably not work with anything else.

The second method is designed for regular software applications. For the program to run it requires that a peripheral device be attached. This makes it much harder to use the software on multiple machines. Inside the dongle is a small microchip that the software program will send signals to. If the dongle is not present then it will not operate. For the software to be used on multiple machines either a copy of the chip inside the dongle would have to be made or the software would have to be modified so that it would not look for the dongle.

One of the main downsides to the use of a dongle is that decreases the usability of the application. Many people would find it inconvenience to have to obtain a dongle every time they wanted to use a certain application. Also if the dongle is lost or damaged the software is rendered useless, and it may not be possible to obtain a replacement without repurchasing the product.

Conclusion

There are many different ways out there that companies try to protect their investment into the software that they produce. None of the methods described above is perfect. It is only a matter of time before any system is cracked. Different methods are right for different products and different companies. Many of the methods on their own are easy to thwart, but when combined they can be a powerful tool to protect a companies assets.

Bibliography

Gold, Steve. "Pirated Copies of Windows XP Pose Security Risk – Microsoft." *Newsbytes* 30 Oct 2001 <http://www.newsbytes.com/cgi-bin/udt/im.display.printable?client.id=newsbytes&story.id=17165> Accessed on 26 Nov. 2001

Lettice, John. "Redmond strives to cram Great MS Hack back in box." *The Register* 8 Nov. 2000 <http://www.theregister.co.uk/content/4/14306.html> Accessed on 26 Nov. 2001

RedHat Corporate Information. Durham, NC. 2001 <http://www.redhat.com/about/corporate/> Accessed on 26 Nov. 2001

Silverman, Dwight. "Microsoft's New Copyright Protection Baldly Insults the Paying Customer." *Pioneer Press* 2 April 2001 <http://www.pioneerpress.com/tech/docs/tech2.htm> Accessed on 26 Nov. 2001

Solidworks Registration FAQ. Concord, MA. 2001 <http://www.solidworks.com/regfaq/regfaq_new_users.cfm> Accessed on 26 Nov. 2001

Microsoft Windows XP Home Edition Product Documentation. Redmond, WA. 2001 <http://www.microsoft.com/windowsxp/home/using/productdoc/en/WPA_overview.asp?frame=true> Accessed on 26 Nov. 2001

WinZip® 8.0 (3105), *WinZip Computing Co*. license agreement/ordering information

---

[1] Lettice, John. "Redmond strives to cram Great MS Hack back in box." *The Register* 8 Nov. 2000 <http://www.theregister.co.uk/content/4/14306.html> Accessed on 26 Nov. 2001

[2] *Solidworks Registration FAQ*. Concord, MA. 2001 <http://www.solidworks.com/regfaq/regfaq_new_users.cfm> Accessed on 26 Nov 2001

[3] WinZip® 8.0 (3105), *WinZip Computing Co*. license agreement/ordering information

[4] *Microsoft Windows XP Home Edition Product Documentation*. Redmond, WA. 2001 <http://www.microsoft.com/windowsxp/home/using/productdoc/en/WPA_overview.asp?frame=true> Accessed on 26 Nov 2001

[5] Gold, Steve. "Pirated Copies of Windows XP Pose Security Risk – Microsoft." *Newsbytes* 30 Oct 2001 <http://www.newsbytes.com/cgi-bin/udt/im.display.printable?client.id=newsbytes&story.id=17165> Accessed on 26 Nov 2001

[6] Silverman, Dwight. "Microsoft's New Copyright Protection Baldly Insults the Paying Customer." *Pioneer Press* 2 April 2001 <http://www.pioneerpress.com/tech/docs/tech2.htm> Accessed on 26 Nov. 2001